Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER

Finite Fields and Their Applications 10 (2004) 432–437

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

On normal integral bases of unramified abelian p-extensions over a global function field of characteristic p

Humio Ichimura

Department of Mathematics, Yokohama City University, 22-2, Seto, Kanazawa-ku, Yokohama 236-0027, Japan

Received 19 July 2002

Communicated by Michael Tsfasman

Abstract

Let K be an algebraic function field of one variable over a finite field of characteristic p, and S a finite non-empty set of prime divisors of K. As the ring of integers of K, we take the ring of elements of K integral outside S. We prove that for a finite abelian p-extension L/K, it has a relative normal integral basis (NIB) if and only if it is unramified outside S. We also give a generator of NIB in an explicit form.

Keywords: Normal integral basis; Function field

1. Introduction

Let p be a fixed prime number, q a power of p, $\boldsymbol{F}_q$ the finite field with q elements, and K an algebraic function field of one variable with constant field $\boldsymbol{F}_q$. Let S be a finite non-empty set of prime divisors of K, and $\mathcal{O}_K = \mathcal{O}_K^S$ the elements of K integral outside S. Let L/K be a finite Galois extension with group G, and let $\mathcal{O}_L = \mathcal{O}_L^S$ be the integral closure of $\mathcal{O}_K$ in L. The extension L/K has a relative normal integral basis (NIB for short) at S when $\mathcal{O}_L = \mathcal{O}_K[G] \cdot \omega$ for some $\omega \in \mathcal{O}_L$. This integer ω is called a generator of NIB. It is well known by Noether that L/K has a NIB at S only when L/K is at most tamely ramified outside S. When G is abelian and $p \nmid |G|$, Chapman

E-mail address: ichimura@yokohama-cu.ac.jp.

1071-5797/$ - see front matter
doi:10.1016/j.ffa.2003.09.006

[4] gave a necessary and sufficient condition for L/K to have a NIB at S in terms of "Kummer generators" of L (under some assumption on S). In this article, we deal with the case where G is an abelian p-group. We prove the following:

Theorem. *Let q, K, S be as above. For a finite abelian p-extension L/K, it has a NIB at S if and only if L/K is unramified outside S.*

The "only if" part is immediate from Noether's theorem.

Let $K = \boldsymbol{F}_q(T)$ be the rational function field with an indeterminate T, and ∞_T the prime divisor of K corresponding to the pole of T. Let Λ_n be the $T^{-(n+1)}$-division points of the Carlitz module $\bar{K}$ over $\boldsymbol{F}_q[1/T]$, and $F_n = K(\Lambda_n)$. Here, $\bar{K}$ is the algebraic closure of K. It is known that F_n/K is an abelian extension of degree $q^n(q-1)$. Let L_n be the unique intermediate field of F_n/K with $[L_n : K] = q^n$. It is known that L_n/K is unramified outside ∞_T and totally ramified at ∞_T. For the Carlitz module and the fields of division points, confer Hayes [9] or Rosen [14, Chapter 12]. Chapman [3, Theorem 5] proved that the unramified p-abelian extension L_n/K has a NIB at $S = \{\infty_T\}$ by explicitly giving a generator of NIB. We show the "if" part of the Theorem in a way similar to the proof of [3, Theorem 5] using Witt vectors in place of Carlitz module.

Remark 1. When $p \nmid |G|$, the "if" part of the Theorem does not hold in general. The reason is as follows. Let ℓ be a prime number with $\ell \neq p$, and assume that $q \equiv 1 \bmod \ell$. Let $h_{K,S}$ be the ideal class number of the Dedekind domain $\mathcal{O}_K^S$. It follows from Greither [8, Proposition **0**.6.5] that if ℓ divides $h_{K,S}$, then there exists a cyclic extension over K of degree ℓ which is unramified outside S and has no NIB at S. There are many examples of (q, K, S, ℓ) with $\ell | h_{K,S}$ (cf. [1,10–12]).

Remark 2. (1) A number field analogue of Chapman's result in [4] is given by Gómez Ayala [7]. (2) Let ℓ be a prime number. Also in the number field case, there are many unramified abelian ℓ-extensions without NIB. For this, see [2,5,13] and some references therein.

2. Proof of the Theorem

Let q, K, S be as in Section 1. Let $L_1, \ldots, L_r$ be cyclic p-extensions over K which are unramified outside S and linearly disjoint over K. Then, the composite $L_1 \cdots L_r/K$ has a NIB at S if each L_i/K has a NIB at S. This is because of a classical theorem on rings of integers in Fröhlich and Taylor [6, III, (2.13)]. Therefore, to show the "if" part of the Theorem, it suffices to deal with cyclic p-extensions over K.

For a commutative ring R of characteristic p with identity, let $W_n(R)$ be the additive group of Witt vectors over R with length $n+1$. When $n = 0$, $W_0(R)$ is nothing but the additive group R. We denote by $\dotplus$ and $\dotminus$ the addition and the subtraction of Witt vectors respectively. Let $[p]$ and $\wp$ be the endomorphisms of

$W_n(R)$ defined by

$$\begin{aligned} [p] &: \boldsymbol{x} = (x_0, \ldots, x_n) \to \boldsymbol{x}^{[p]} = (x_0^p, \ldots, x_n^p), \\ \wp &: \boldsymbol{x} \to \wp(\boldsymbol{x}) = \boldsymbol{x}^{[p]} \dot{-} \boldsymbol{x}, \end{aligned}$$

respectively.

Let q, K, S be as in Section 1. For brevity, we write $\mathcal{O}_K = \mathcal{O}_K^S$ and $\mathcal{O}_L = \mathcal{O}_L^S$ for a finite extension L/K. For a Witt vector $\boldsymbol{a} = (a_0, \ldots, a_n) \in W_n(K)$, let $\boldsymbol{a}^{1/\wp} = \boldsymbol{x} = (x_0, \ldots, x_n)$ be an element of $W_n(\bar{K})$ satisfying the equation $\wp(\boldsymbol{x}) = \boldsymbol{a}$. Let $L = K(\boldsymbol{a}^{1/\wp}) = K(x_0, \ldots, x_n)$. This is a cyclic extension over K. It is of degree p^{n+1} if and only if $a_0 \notin \wp(K)$, and when this is the case, the Galois group $\mathrm{Gal}(L/K)$ is generated by the automorphism sending $\boldsymbol{x}$ to $\boldsymbol{x} \dot{+} (1, 0, \ldots, 0)$.

The Theorem follows from the following two propositions. The second one is given in [15, p. 162].

Proposition 1. *Let $\boldsymbol{a} = (a_0, \ldots, a_n) \in W_n(\mathcal{O}_K)$ be a Witt vector with $a_0 \notin \wp(\mathcal{O}_K)$. Let $\boldsymbol{x} = \boldsymbol{a}^{1/\wp} = (x_0, \ldots, x_n)$, $L = K(\boldsymbol{x})$, and*

$$\omega_n = \left(\prod_{i=0}^{n} x_i \right)^{p-1}.$$

Then, the cyclic extension L/K of degree p^{n+1} is unramified outside S, and has a NIB at S. More precisely, we have $\omega_n \in \mathcal{O}_L$ and $\mathcal{O}_L = \mathcal{O}_K[G] \cdot \omega_n$, where $G = \mathrm{Gal}(L/K)$.

Proposition 2. *Let L/K be a cyclic extension of degree p^{n+1} unramified outside S. Then, we have $L = K(\boldsymbol{a}^{1/\wp})$ for some $\boldsymbol{a} = (a_0, \ldots, a_n) \in W_n(\mathcal{O}_K)$ with $a_0 \notin \wp(\mathcal{O}_K)$.*

3. Proof of Proposition 1

First, let us recall how the addition of Witt vectors is defined. Let X_i, Y_i $(0 \leqslant i \leqslant n)$ be variables, and define a polynomial W_n in $\boldsymbol{Z}[X_0, \ldots, X_n]$ by

$$\begin{aligned} W_n(X_0, \ldots, X_n) &= \sum_{i=0}^{n} p^i X_i^{p^{n-i}} \\ &= X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^{n-1} X_{n-1}^p + p^n X_n. \end{aligned}$$

For each i with $0 \leqslant i \leqslant n$, there uniquely exists a polynomial

$$\sigma_i = \sigma_i(X_0, \ldots, X_n; Y_0, \ldots, Y_n) \in \boldsymbol{Z}[X_0, \ldots, X_n, Y_0, \ldots, Y_n]$$

satisfying

$$W_n(\sigma_0, \ldots, \sigma_n) = W_n(X_0, \ldots, X_n) + W_n(Y_0, \ldots, Y_n).$$

From the above, we easily see that

$$\sigma_n \equiv X_n + Y_n \bmod \boldsymbol{Z}[X_0, \ldots, X_{n-1},\ Y_0, \ldots, Y_{n-1}]. \tag{1}$$

For a commutative ring R of characteristic p with identity, the addition on $W_n(R)$ is defined by

$$\boldsymbol{a} \dotplus \boldsymbol{b} = (\sigma_0(a_0,\ b_0), \ldots, \sigma_n(a_0, \ldots, a_n; b_0, \ldots, b_n))$$

for $\boldsymbol{a} = (a_0, \ldots, a_n)$, $\boldsymbol{b} = (b_0, \ldots, b_n) \in W_n(R)$.

Let q, K, S, $\mathcal{O}_K = \mathcal{O}_K^S$ be as in Section 1, and we use the same notation as in Sections 1, 2.

Lemma 1. *Let $a \in \mathcal{O}_K \backslash \wp(\mathcal{O}_K)$, $x = a^{1/\wp}$, and $L = K(x)$. Let $G = \mathrm{Gal}(L/K)$, and σ be a generator of the cyclic group G of order p. Then, L/K is unramified outside S, and*

$$\mathcal{O}_L = \mathcal{O}_K[x] = \mathcal{O}_K[G] \cdot x^{p-1}.$$

Further, the integers $1, x, \ldots, x^{p-1}$ are written as linear combinations of $x^{p-1}, (x^{p-1})^{\sigma}, \ldots, (x^{p-1})^{\sigma^{p-1}}$ with coefficients in $\boldsymbol{F}_p$.

Proof. By the definition, x is a root of $f(X) = X^p - X - a \in \mathcal{O}_K[X]$. As $f'(X) = -1$, we see that L/K is unramified outside S, and that

$$\mathcal{O}_L = \mathcal{O}_K[x] = \bigoplus_{j=0}^{p-1} \mathcal{O}_K x^j.$$

To show $\mathcal{O}_L = \mathcal{O}_K[G] \cdot x^{p-1}$, it suffices to show the last assertion of the lemma. We may as well assume that σ sends x to $x+1$. Then, we have

$$(x^{p-1})^{\sigma^i} = (x+i)^{p-1} = \sum_{j=0}^{p-1} {}_{p-1}C_j i^{p-1-j} x^j.$$

Let X be the $p \times p$-matrix whose (i, j)-component equals ${}_{p-1}C_j i^{p-1-j}$ with $0 \leqslant i, j \leqslant p-1$. It follows from the above that

$${}^t(x^{p-1},\ (x^{p-1})^{\sigma}, \ldots, (x^{p-1})^{\sigma^{p-1}}) = X \cdot {}^t(1,\ x, \ldots, x^{p-1}).$$

Here, ${}^t(*)$ means the transpose of a matrix. We easily see that the determinant of X equals

$$|X| = \prod_{j=0}^{p-1} {}_{p-1}C_j \times \prod_{0 \leqslant i < j \leqslant p-1} (j-i),$$

and hence $|X| \in \boldsymbol{F}_p^{\times}$. From this, the assertion follows. □

Proof of Proposition 1. Let $\boldsymbol{a} = (a_0, \ldots, a_n)$ be a Witt vector in $W_n(\mathcal{O}_K)$ with $a_0 \notin \wp(\mathcal{O}_K)$, and $\boldsymbol{x} = (x_0, \ldots, x_n)$ a root of $\wp(\boldsymbol{x}) = \boldsymbol{a}$. Let $L_{-1} = K$, and $L_i = K(x_0, \ldots, x_i)$ for $0 \leqslant i \leqslant n$. Denote by $\mathcal{O}_i = \mathcal{O}_{L_i}^S$ the ring of integers of L_i. We see that $x_i \in \mathcal{O}_i$, and that for $0 \leqslant i \leqslant n$,

$$x_i^p = x_i + a_i + b_i \tag{2}$$

for some $b_i \in \mathcal{O}_{i-1}$ by the formula (1). Then, it follows from Lemma 1 that L_i/L_{i-1} is unramified outside S, and hence so is L_n/K. It also follows from Lemma 1 that

$$\mathcal{O}_i = \mathcal{O}_{i-1}[x_i] = \bigoplus_{j=0}^{p-1} \mathcal{O}_{i-1} x_i^j. \tag{3}$$

Let $G = \mathrm{Gal}(L_n/K)$ and $H = \mathrm{Gal}(L_n/L_{n-1})$. We show $\mathcal{O}_n = \mathcal{O}_K[G] \cdot \omega_n$ by induction on n. So, let us assume that

$$\mathcal{O}_{n-1} = \mathcal{O}_K[G/H] \cdot \omega_{n-1} \quad \text{with } \omega_{n-1} = \left(\prod_{i=0}^{n-1} x_i \right)^{p-1}. \tag{4}$$

To show $\mathcal{O}_n = \mathcal{O}_K[G] \cdot \omega_n$, it suffices to show that

$$\mathcal{O}_{n-1} x_n^j \subseteq \mathcal{O}_K[G] \cdot \omega_n \quad \text{for } 0 \leqslant j \leqslant p-1 \tag{5}$$

because of (3). Let us show this by induction on j. By Lemma 1 and (2) with $i = n$, the elements $1, x_n, \ldots, x_n^{p-1}$ are linear combinations of $(x_n^{p-1})^\tau$ $(\tau \in H)$ with coefficients in $\boldsymbol{F}_p$. Therefore, as $\omega_n = \omega_{n-1} x_n^{p-1}$, we see that

$$\omega_{n-1},\ \omega_{n-1} x_n, \ldots, \omega_{n-1} x_n^{p-1} \in \mathcal{O}_K[H] \cdot \omega_n \subseteq \mathcal{O}_K[G] \cdot \omega_n. \tag{6}$$

In particular, assertion (5) holds when $j = 0$ because of the assumption (4). Let J be an integer with $0 \leqslant J \leqslant p-2$, and assume that (5) holds for all j with $0 \leqslant j \leqslant J$;

$$A_J := \bigoplus_{j=0}^{J} \mathcal{O}_{n-1} x_n^j \subseteq \mathcal{O}_K[G] \cdot \omega_n. \tag{7}$$

Let σ be the generator of the cyclic Galois group G sending the Witt vector $\boldsymbol{x}$ to $\boldsymbol{x} + (1, 0, \ldots, 0)$. Then, we have $x_n^{\sigma^k} \equiv x_n \bmod \mathcal{O}_{n-1}$ by (1). From this, we see that

$$(\omega_{n-1} x_n^{J+1})^{\sigma^k} \equiv \omega_{n-1}^{\sigma^k} x_n^{J+1} \bmod A_J.$$

By (7), this congruence also holds modulo $\mathcal{O}_K[G] \cdot \omega_n$. By (6), $\omega_{n-1} x_n^{J+1}$ is contained in $\mathcal{O}_K[G] \cdot \omega_n$. Hence, so is the conjugate $(\omega_{n-1} x_n^{J+1})^{\sigma^k}$. Therefore, we obtain $\omega_{n-1}^{\sigma^k} x_n^{J+1} \in \mathcal{O}_K[G] \cdot \omega_n$ by the above congruence. From this and assumption (4), we see that $\mathcal{O}_{n-1} x_n^{J+1} \subseteq \mathcal{O}_K[G] \cdot \omega_n$. Thus, we have shown assertion (5). □

Acknowledgments

The author was partially supported by Grant-in-Aid for Scientific Research (C) (No. 13640036), the Ministry of Education, Culture, Sports, Science and Technology of Japan.

References

[1] B. Angles, On the class group problem for function fields, J. Number Theory 70 (1998) 146–159.
[2] J. Brinkhuis, Unramified abelian extensions of CM-fields and their Galois module structure, Bull. London Math. Soc. 24 (1992) 236–242.
[3] R.J. Chapman, Carlitz modules and normal integral bases, J. London Math. Soc. 44 (1991) 250–260.
[4] R.J. Chapman, Kummer theory and Galois module structure in global function fields, Math. Zeit. 208 (1991) 375–388.
[5] L.N. Childs, The group of unramified Kummer extensions of prime degree, Proc. London Math. Soc. 35 (1977) 407–422.
[6] A. Fröhlich, M.J. Taylor, Algebraic Number Theory, Cambridge University Press, Cambridge, 1991.
[7] E.J. Gómez Ayala, Bases normales d'entiers dans les extensions de Kummer de degré premier, J. Theor. Nombres Bordeaux 6 (1994) 95–116.
[8] C. Greither, Cyclic Galois Extensions of Commutative Rings, in: Lecture Notes in Mathematics, Vol. 1534, Springer, Berlin, Heidelberg, New York, 1992.
[9] D.R. Hayes, Explicit class field theory for rational function fields, Trans. Amer. Math. Soc. 189 (1974) 77–91.
[10] H. Ichimura, On the class group of pure function fields, Proc. Japan Acad. 64A (1988) 170–173 Corrigendum 75A (1999) 22.
[11] H. Ichimura, On the class numbers of the maximal real subfields of cyclotomic function fields, Finite Fields Appl. 4 (1998) 167–174.
[12] H. Ichimura, On the class numbers of the maximal real subfields of cyclotomic function fields, II, J. Number Theory 72 (1998) 140–149.
[13] H. Ichimura, H. Sumida, A note on integral bases of unramified cyclic extensions of prime degree. II, Manuscripta Math. 104 (2001) 201–210.
[14] M. Rosen, Number Theory in Function Fields, in: Graduate Texts in Mathematics, Vol. 210, Springer, Berlin, Heidelberg, New York, 2001.
[15] L. Schmid, Zur Arithmetik der Zyklischen p-Körper, J. Reine Angew. Math. 176 (1937) 161–167.